

Nos. 19-MJ-4207-DHH, 19-MJ-4208-DHH, and 19-MJ-4209-DHH

AFFIDAVIT

I, Special Agent David F. Simmons, depose and state as follows:

1. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”), and have been so employed since 2015. I am currently assigned to the Boston Field Division’s Bridgewater Field Office in Bridgewater, Massachusetts, and was previously assigned to the Miami Field Division in Doral, Florida. Prior to becoming a Special Agent with ATF, I was employed as a Police Officer within the Commonwealth of Massachusetts for approximately nine years. During this time, I spent approximately one year as a detective, where I investigated various offenses, including narcotics offenses, and received training in conducting advanced criminal investigations.

2. As a Special Agent for ATF, some of my duties include: conducting criminal investigations into cases of illegal possession/transfer of firearms, firearms trafficking, and violent crimes involving firearms and narcotics trafficking. Through my training, knowledge, and experience, I have become familiar with the habits, methods, routines, practices and procedures commonly employed by persons engaged in the use and trafficking of illegal firearms. I have been the affiant on numerous affidavits in support of federal and state search warrants, arrest warrants, and other applications. I have participated in and performed surveillance and made arrests of firearm and narcotics traffickers who utilize their electronic devices to further their illegal activity. During the course of my professional experience, I have interviewed numerous defendants, witnesses, victims, confidential informants, and other police officers regarding the illegal trafficking of firearms and narcotics.

3. I submit this affidavit in support of application for the following search warrants:

- a. To search electronic equipment, specifically the following mobile phone: Motorola phone, Model # XT1921-2, IMEI: 359542090438837 (“Target Device 1”) that is in possession of ATF, located at 1 Lakeshore Center, Bridgewater, Massachusetts 02324, as further described in Attachment A-1. This phone was seized by Massachusetts State Police during the arrest of DIOVANNI CARTER on a state warrant charging him with the armed robbery taking place on 1/26/19.
 - b. To search electronic equipment, specifically the following mobile phone: Black iPhone with red case (“Target Device 2”) that is in possession of ATF, located at 1 Lakeshore Center, Bridgewater, Massachusetts 02324, as further described in Attachment A-2. This phone was seized during the execution of search warrants at 82 Carl Avenue, Brockton, MA. JAMES BODDIE is the user of this phone.
 - c. To search electronic equipment, specifically the following mobile phone: Black iPhone with red case (“Target Device 3”) that is in possession of ATF, located at 1 Lakeshore Center, Bridgewater, Massachusetts 02324, as further described in Attachment A-2. This phone was seized during the execution of search warrants at 82 Carl Avenue, Brockton, MA. JAMES BODDIE is the user of this phone.
4. Collectively, Target Device 1, Target Device 2, and Target Device 3 will be referred to as the Target Devices or the equipment.
5. The statements contained in this affidavit are based on my own investigation and on documents, and information provided to me by officers of the Brockton Police Department (“BPD”), Massachusetts State Police (“MSP”) and Plymouth County Sheriff Department (“PCSD”). This affidavit is submitted for the limited purpose of establishing probable cause and therefore does not set forth all of the information that I and other law enforcement personnel have obtained during the course of this investigation.
6. This affidavit incorporates by reference a signed affidavit, sworn and submitted in support of prior search warrant applications, 19-MJ-4148, 4149, and 4152. This affidavit is attached as an exhibit to the instant affidavit, and the facts contained therein should be considered incorporated within this affidavit. As such, this affidavit does not set forth the factual information concerning the underlying crime because that information contained in the attached affidavit, Exhibit 1.

I. TARGET PHONE 1: ARREST OF DIOVANNI CARTER

7. On March 5, 2019, DIOVANNI CARTER was arrested by MSP on the outstanding state warrant charging him with the January 26, 2019, armed robbery and firearm offenses. Target Device 1 seized incident to the arrest of DIOVANNI CARTER.

8. It is my understanding that DIOVANNI CARTER was located by MSP Troopers through a state court search warrant for a ping order on the phone associated with the phone number 508-577-6720, serviced by AT&T Wireless. I have reviewed the affidavit submitted by Trooper John Sullivan in support of the ping order for the 508-577-6720 phone.

9. In the affidavit, Trooper Sullivan reported that MSP developed the attribution of the 508-577-6720 phone to DIOVANNI CARTER through analysis of other known contacts of DIOVANNI CARTER, including contact between the 508-577-6720 phone and relatives of DIOVANNI CARTER and the 508-408-3998 phone used by JAMES BODDIE. The 508-577-6720 phone made contact with known contacts of DIOVANNI CARTER and was then determined to be his phone. Target Device 1 bears the logo of AT&T on the back.

10. Records received on March 15, 2019, from AT&T for the 508-577-6720 number associated the 508-577-6720 phone number with the IMEI #:359542090438837. The subscriber listed for the account is Nancy Carter, of 108 Moraine Street, Brockton, MA.

11. According to records received from the Plymouth County Sheriff's Department, DIOVANNI CARTER listed Nancy Carter as his grandmother on papers filed March 7, 2019.

12. As such, I believe that Target Device 1 is in fact the device associated with the 508-577-6720 phone number, and that DIOVANNI CARTER is the user of Target Device 1.

13. I have reviewed the call detail records of the 508-408-3998 phone for which BODDIE is the believed the user. Those records were for the period of 1/5/19 through 2/20/19. Review of

those records revealed that there were multiple calls between the 508-577-6720 phone and the 508-408-3998 phone on 2/11/19 and 2/20/19, suggesting that BODDIE and DIOVANNI CARTER were in contact while DIOVANNI CARTER was in warrant status.

II. TARGET PHONE 2 AND TARGET PHONE 3

14. On March 13, 2019, the ATF, Brockton Police Department, and the Massachusetts State Police executed federal search warrants at 82 Carl Street Brockton, Massachusetts. Upon making entry to the residence, law enforcement officers encountered multiple individuals, including James BODDIE and the girlfriend of BODDIE, located in the front left bedroom. BODDIE was detained by law enforcement as he was exiting the bed located in this bedroom while the girlfriend was detained still on the bed.

15. Upon detaining BODDIE, investigators identified two cellular telephones on the headboard above the pillow of BODDIE and one gold colored cellular telephone on the headboard above the girlfriend of BODDIE. The two cellular telephones above BODDIE were black Apple iPhone model phones with black and red cases. A photograph of the two iPhones follows:



16. Law enforcement then located a clear glassine bag under the pillow located on the portion of the bed formerly occupied by BODDIE. Within this clear glassine bag, investigators observed five knotted plastic bags containing a rock like white substance consistent, with my training and

experience, to be cocaine base, also known as crack cocaine. Next to the clear glassine bag containing the knotted glassine bags, investigators located a straw and \$40 of United States currency. \$35 was found in BODDIE's wallet. The white substance was field tested and the test indicated the presence of cocaine base. The cocaine base was weighed to be 2.5 grams.

17. Next to the bed on the side once occupied by BODDIE, law enforcement observed multiple shoeboxes and a paper bag which contained plastic sandwich bags, and a pair of scissors consistent with narcotics distribution. Law enforcement also observed a digital scale within the dresser at the foot of the bed occupied by BODDIE in the top right drawer.

18. It should be noted, prior to the execution of the federal search warrant, the Brockton Police Department Narcotics Unit had an active investigation into BODDIE. This investigation included two separate controlled purchases of crack cocaine from BODDIE utilizing a confidential informant.¹ One of these controlled purchases took place at 82 Carl Street in Brockton, Massachusetts, on January 18, 2019. The other controlled purchase came from BODDIE while he operated a gray 2011 Honda Accord bearing Massachusetts Registry of Motor Vehicles license plate number 8NC799, on February 26, 2019.

19. During the course of the searches, agents located a grey Nike sweatshirt with a white logo on the left breast, a pair of grey Nike sweatpants, and white Nike sneakers, consistent with the clothing worn by BODDIE at 2:21 PM on 1/26/19 at the T-Mobile store.

20. I have reviewed the criminal history and criminal convictions of BODDIE and determined

¹ The CI used in this investigation has a criminal record consisting of arrests for assault and battery, providing a false name, malicious destruction of property, felony larceny, and violation of an abuse prevention order, shoplifting, assault and battery by means of a dangerous weapon. The CI is receiving monetary benefits. The CI is not receiving any consideration on active criminal cases.

BODDIE to have been convicted of the following:

- Possession of Cocaine, Plymouth Superior Court Docket #1783CR00112B, (originally charged with possession with intent, subsequent offense, convicted of lesser included offense);
- Felon in Possession of a Firearm, Boston Federal Court Docket #111038201;
- Possession of Controlled Substance Cocaine, Plymouth Superior Court Docket #1000690001;
- Possession Of Firearm without FID Card, Brockton District Court #0718CR009326B;
- Possession Class B Controlled Substance Crack Cocaine, Brockton District Court Docket #0715CR009326D;
- Distribution/Class B Cocaine, Brockton District Court Docket #0515CR007994A; and
- Possession Class B Controlled Substance, Brockton District Court Docket #0415CR004864A.

III. DRUG DISTRIBUTION PRACTICES

21. Based upon my training and experience conducting investigations of drug trafficking organizations, I know that there are common practices employed by drug traffickers in the course of their illicit business. Specifically, drug traffickers commonly keep mobile telephones to be used to contact and receive correspondence from drug sources of supply, gun sources of supply, co-conspirators and associates, and drug customers. In the course of conducting their business, drug traffickers are required to conduct their communications on multiple occasions on a daily basis. The correspondence that drug traffickers are required to maintain on their mobile telephone results in substantial evidence of drug trafficking activity being maintained in their telephone as it pertains to date, time, and duration of illegal drug-trafficking related communications. These communications often occur in a variety of ways, which include, but are not limited to text messaging (often used in lieu of phone call to avoid speaking over the telephone), WhatsApp

messenger, e-mails, “SnapChat” messaging, Instagram, and Facebook messaging. Contents of these communications often denote locations, dates and times of prearranged meetings between sources of drug supply, co-conspirators and associates, and drug customers, drug types and amounts, and prices agreed upon. Moreover, telephone numbers and corresponding identities are often stored in drug trafficker’s mobile telephone to facilitate these routine communications.

22. In short, these communications result in records stored within the mobile phone which contain details of the mobile phone owner’s drug trafficking activities. Based upon the controlled purchases described above conducted by Brockton Police, I know that BODDIE used a mobile phone to arrange at least two drug transactions.

23. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

IV. TECHNICAL INFORMATION CONCERNING PHONE EXTRACTIONS

24. As discussed above, the Target Devices were seized during the arrest of DIOVANNI CARTER and the execution of search warrants. From my training and experience and the training and experience of law enforcement personnel who routinely handle this equipment, I understand that the Target Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when they first came into the investigators’ possession.

25. Based on my training, experience, and information provided by other law enforcement officers, I know that many smartphones (which are included in Attachment B-1 and, B-2’s

definition of “hardware”) can now function essentially as small computers. Apple and Motorola brand phones, such as the Target Devices, are a type of smartphone. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data both on the device itself and online through cloud storage services offered by the software providers. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, and evidence of devices historically used by the user.

26. Based on my knowledge, training, experience, and information provided to me by other agents, I know that data can often be recovered months or even years after it has been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their electronic equipment, they can easily transfer the data from their old device to a new one.
- b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file often does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, the device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, electronic storage media often contains electronic evidence of how the device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but users typically do not erase or delete this evidence because special software is typically required for that task.
- d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

27. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computer equipment to carry out, communicate about, and store records regarding their daily activities. These tasks are frequently accomplished through sending and receiving e-mail, instant messages, and other forms of phone or internet based messages; scheduling activities; keeping a calendar of activities; arranging travel; purchasing items; searching for information including information regarding travel and activities; arranging for travel, accessing personal accounts including banking information; paying for items; and creating and storing images and videos of their movements and activities. These types of information and evidence of certain uses can be present on a smartphone even if the user acquired the actual device after the activity generating the information because user data, such as documents, contacts, messages, emails, and places of interest, are routinely transmitted and stored for the user through online services, such as Google's GMAIL and Google Drive and Apple's iCloud that are linked to the smartphone. When a user changes smartphones, they are able to obtain the historical data and information from the online account storage, use that data and information on the new device.

28. For the Hobbs Act robbery of the T-Mobile store currently under investigation, I would expect evidence of preparation and planning to be stored in the Target Devices. In particular, the suspects are believed to live in Boston and travelled specifically to Brockton, MA, in order to commit the crime, and made calls to plan and commit the crime. Additionally, I am aware the conspiracy obtained the use of the white Malibu that was rented from Hertz and paid for using a credit card. Such activity incident to the coordination, communication, preparation and planning of a crime can be reflected in the data stored on a smart phone through emails, text messages, call logs, searched-for items, navigation applications, photographs, mapping applications, and websites visited.

29. For BODDIE's drug distribution crimes, in violation of 21 U.S.C. 841(a)(1), I would expect evidence of communications, calls, photographs, text messages, call detail records, of the drug distribution activities. Such communications include discussions of price, drug amounts, drug types, coordination of sales made by BODDIE, and purchases of product by BODDIE from his supplier.

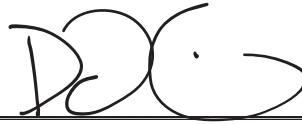
CONCLUSION

30. Based on the information described above, and in the incorporated Affidavit, Exhibit 1, there is probable cause to believe that DIOVANNI CARTER, DARIUS CARTER, STEPHAN ROSSER-STEWART, DENNIS MARTIN, and JAMES BODDIE have violated 18 U.S.C. § 1951(a), through the commission of a robbery that affected interstate commerce and conspiracy to commit a robbery to commit that offense. Additionally, based on the information described above, there is probable cause to believe that JAMES BODDIES has violated 21 U.S.C. §§ 841(a)(1), and 846 by possessing cocaine base with the intent to distribute, and conspiring to commit that offense.

31. Based on the information described above, and in the incorporated Affidavit, Exhibit 1, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 922(g)(1), 1951(a), further described in Attachments B-1, will be found in Target Device 1, as further described in Attachment A-1.

32. Based on the information described above, and in the incorporated Affidavit, Exhibit 1, there is probable cause to believe that evidence of violations of 18 U.S.C. § 1951(a), and 21 U.S.C. §§ 841(a)(1), 846, further described in Attachments B-2, will be found in Target Device 2 and Target Device 3, as further described in Attachments A-2.

Signed under the pains and penalties of perjury this 19th day of March, 2019.



Special Agent David F. Simmons
Bureau of Alcohol, Tobacco, Firearms and Explosives

Subscribed and sworn to before me this 19th day of March, 2019.



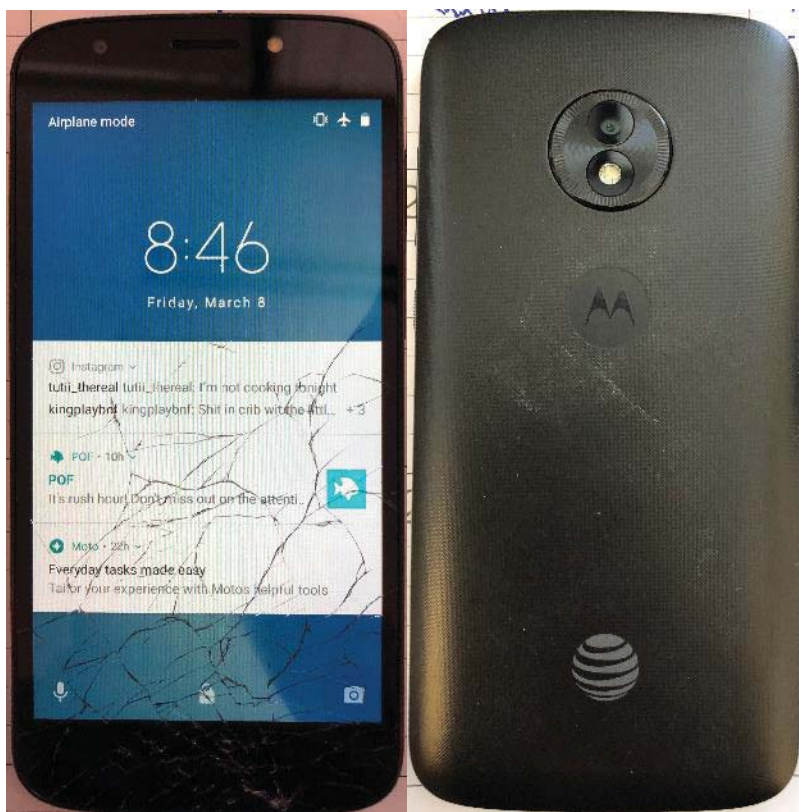
HON. DAVID H. HENNESSEY
CHIEF UNITED STATES DISTRICT JUDGE



ATTACHMENT A-1

The equipment to be searched consists of the following: Motorola phone, Model # XT1921-2, IMEI: 359542090438837 (“Target Device 1” or the “equipment”). Target Device 1 that is in possession of ATF, located at 1 Lakeshore Center, Bridgewater, Massachusetts 02324, as further described in Attachment A-1.

Images of the phone are included below:



ATTACHMENT B-1

- I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. §§ 922(g)(1), and 1951(a), including those related to:
- A. Communications, discussion, planning for and preparation of robberies, including selection of targets, familiarity with roads and means of access, procurement of transportation, procurement of weapons and ammunition, the disposition and monetization of stolen items;
 - B. The identities, aliases, addresses, email addresses, whereabouts, and telephone numbers, of conspirators and other persons furthering the conspiracy;
 - C. Possession of firearms and ammunition;
 - D. The locations of meetings and other aspects of the conspiracy, including where the conspiracy was formed and was furthered, weapons and ammunition were obtained, the crime committed, and where suspects intended to flee;
 - E. The methods of communications between conspirators and associates, including the telephone numbers, messaging applications, and social media accounts used by conspirators;
 - F. The substance of communications regarding criminal activities, including discussions regarding firearms, ammunition, robberies, and any acts of violence;
 - G. The identity, location, and travel or historical whereabouts of any conspirators or associates, as well as any acts taken in furtherance of the crimes listed above;
 - H. Evidence of who used, owned, or controlled the equipment;
 - I. Evidence of malicious computer software that would allow others to control the equipment, software, or storage media, evidence of the lack of such malicious

software, and evidence of the presence or absence of security software designed to detect malicious software;

- J. Evidence of the attachment of other hardware or storage media;
 - K. Evidence of counter-forensic programs and associated data that are designed to eliminate data;
 - L. Evidence of the times the equipment was used;
 - M. Passwords, encryption keys, and other access devices that may be necessary to access the equipment; and
 - N. Records relating to accounts held with companies providing Internet access or remote storage of either data or storage media.
- II. Serial numbers and any electronic identifiers that serve to identify the computer equipment.

DEFINITIONS

For the purpose of this warrant:

- A. “Equipment” means any hardware, software, storage media, and data.
- B. “Hardware” means any electronic device capable of data processing (such as a computer, digital camera, cellular telephone or smartphone, wireless communication device, or GPS navigation device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. “Software” means any program, program code, information or data stored in any

form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

- D. “Storage media” means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).
- E. “Data” means all information stored on storage media of any form in any storage format and for any purpose.
- F. “A record” is any communication, representation, information or data. A “record” may be comprised of letters, numbers, pictures, sounds or symbols.

Return of Seized Equipment

If, after inspecting seized equipment, the government determines that the equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy’s authenticity and accuracy (but not necessarily relevance or admissibility) for evidentiary purposes.

If equipment cannot be returned, agents will make available to the equipment’s owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, personally-identifying information of victims; or the fruits or instrumentalities of crime.

ATTACHMENT A-2

The equipment to be searched consists of the following: a Black iPhone with red case (“Target Device 2”) that is in possession of ATF, located at 1 Lakeshore Center, Bridgewater, Massachusetts 02324; and a Black iPhone with red case (“Target Device 3”) that is in possession of ATF, located at 1 Lakeshore Center, Bridgewater, Massachusetts 02324. Collectively, Target Device 2 and Target Device 3 will be referred to as the “equipment” or the “Target Devices.”

A photograph of Target Device 2 and Target Device 3 follows:



ATTACHMENT B-2

I. All records, in whatever form, and tangible objects that constitute evidence, or instrumentalities of 18 U.S.C. § 1951(a), and 21 U.S.C. §§ 841(a)(1), and 846 including those related to:

- A. Communications, discussion, planning for and preparation of robberies, including selection of targets, familiarity with roads and means of access, procurement of transportation, procurement of weapons and ammunition, the disposition and monetization of stolen items;
- B. The identities, aliases, addresses, email addresses, whereabouts, and telephone numbers, of conspirators and other persons furthering the conspiracy;
- C. Possession of firearms and ammunition;
- D. Possession and distribution of controlled substances, including fentanyl, heroin, cocaine, cocaine base a/k/a crack cocaine, and marijuana,
- E. The locations of meetings and other aspects of the conspiracy, including where the conspiracy was formed and was furthered, weapons and ammunition were obtained, the crime committed, and where suspects intended to flee;
- F. The methods of communications between conspirators and associates, including the telephone numbers, messaging applications, and social media accounts used by conspirators;
- G. The communications regarding discussions regarding purchase, sale and distribution of controlled substances, prices, locations of sales, individuals who purchased controlled substances, individuals who sold controlled substances, and any sources of supply of controlled substances;

- H. The identity, location, and travel or historical whereabouts of any conspirators or associates, as well as any acts taken in furtherance of the crimes listed above;
 - I. Evidence of who used, owned, or controlled the equipment;
 - J. Evidence of malicious computer software that would allow others to control the equipment, software, or storage media, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;
 - K. Evidence of the attachment of other hardware or storage media;
 - L. Evidence of counter-forensic programs and associated data that are designed to eliminate data;
 - M. Evidence of the times the equipment was used;
 - N. Passwords, encryption keys, and other access devices that may be necessary to access the equipment; and
 - O. Records relating to accounts held with companies providing Internet access or remote storage of either data or storage media.
- II. Serial numbers and any electronic identifiers that serve to identify the computer equipment.

DEFINITIONS

For the purpose of this warrant:

- A. “Equipment” means any hardware, software, storage media, and data.
- B. “Hardware” means any electronic device capable of data processing (such as a computer, digital camera, cellular telephone or smartphone, wireless communication device, or GPS navigation device); any peripheral input/output

device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

- C. “Software” means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.
- D. “Storage media” means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).
- E. “Data” means all information stored on storage media of any form in any storage format and for any purpose.
- F. “A record” is any communication, representation, information or data. A “record” may be comprised of letters, numbers, pictures, sounds or symbols.

Return of Seized Equipment

If, after inspecting seized equipment, the government determines that the equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy’s authenticity and accuracy (but not necessarily relevance or admissibility) for evidentiary purposes.

If equipment cannot be returned, agents will make available to the equipment's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, personally-identifying information of victims; or the fruits or instrumentalities of crime.